Fig. 1

PRP-Privacy Reference Points
Virtual Chip Cards
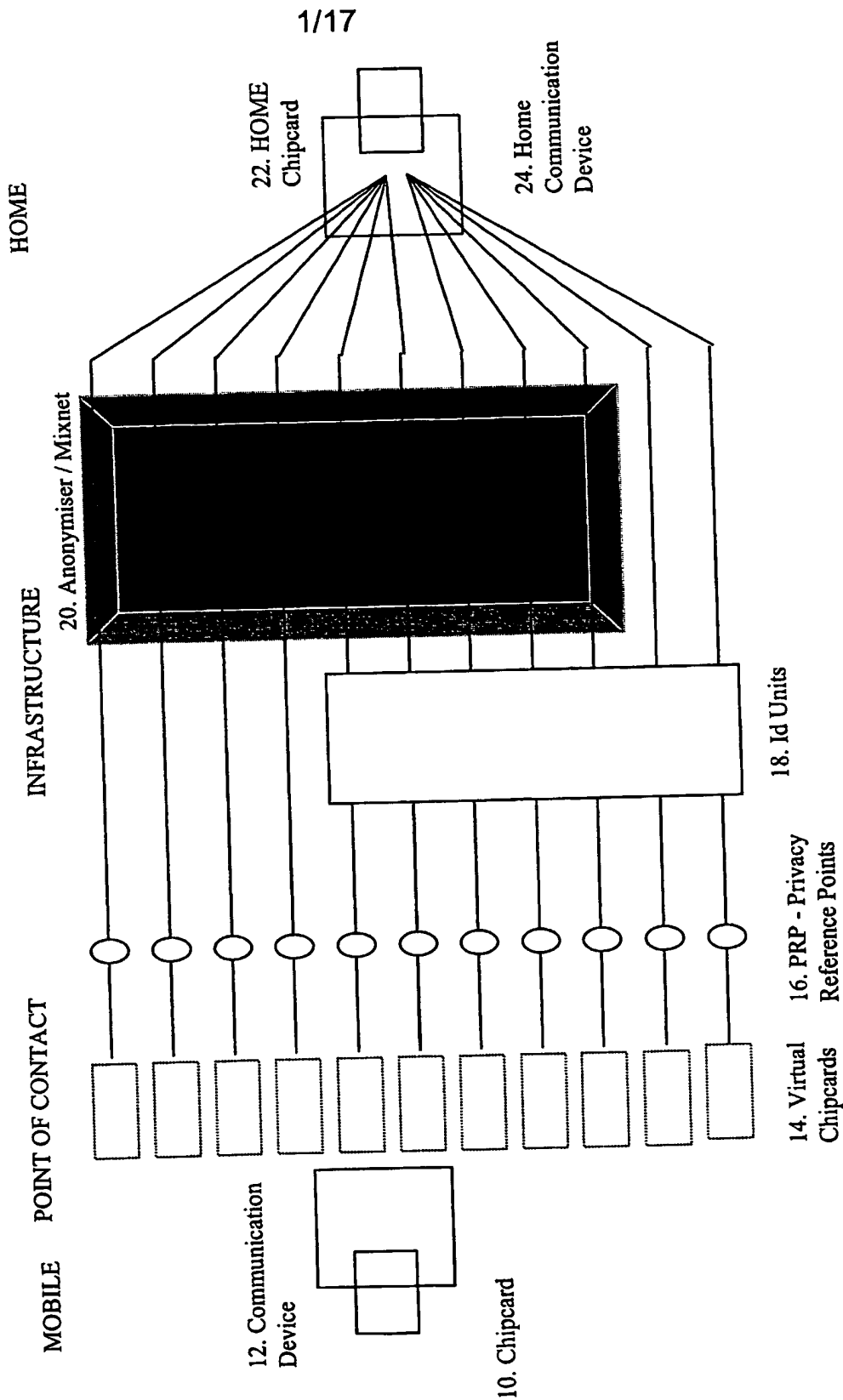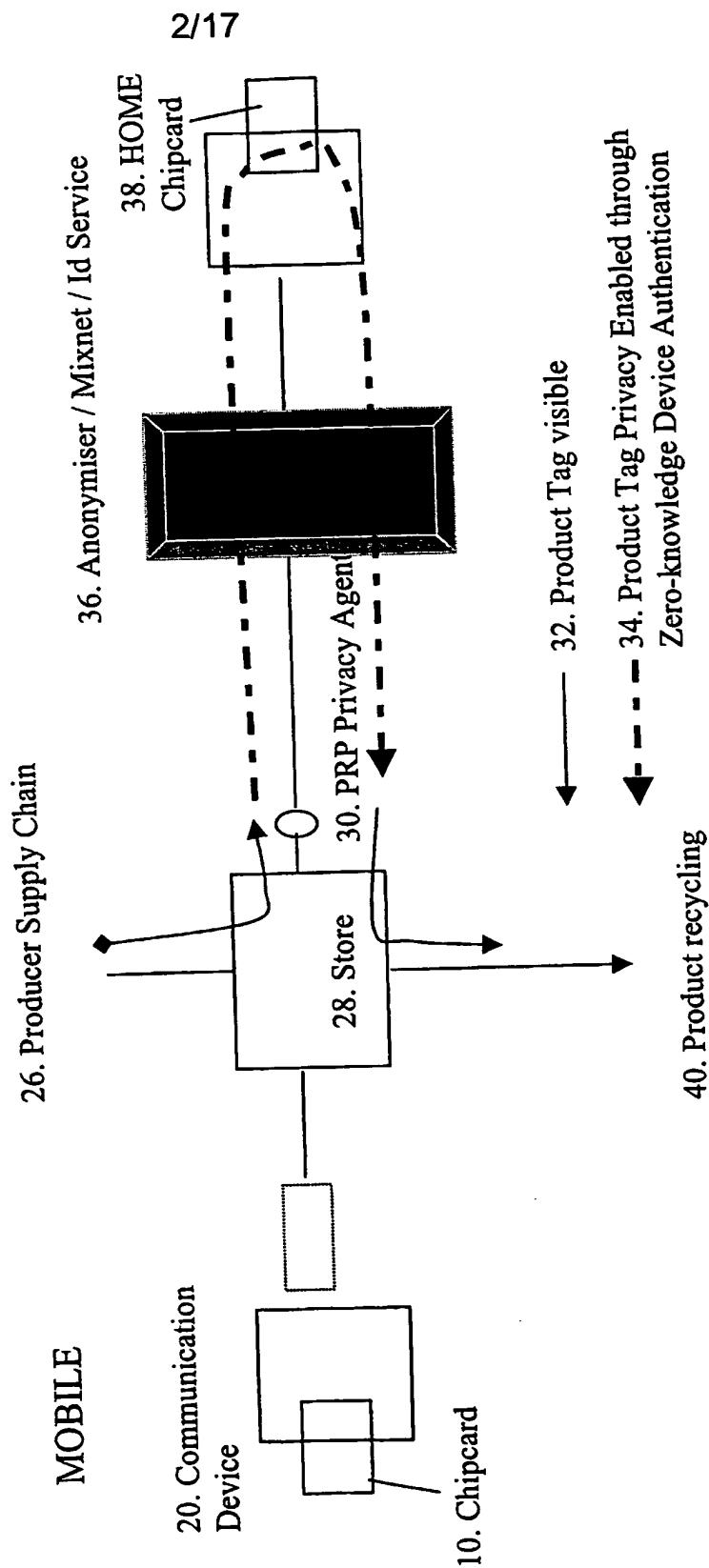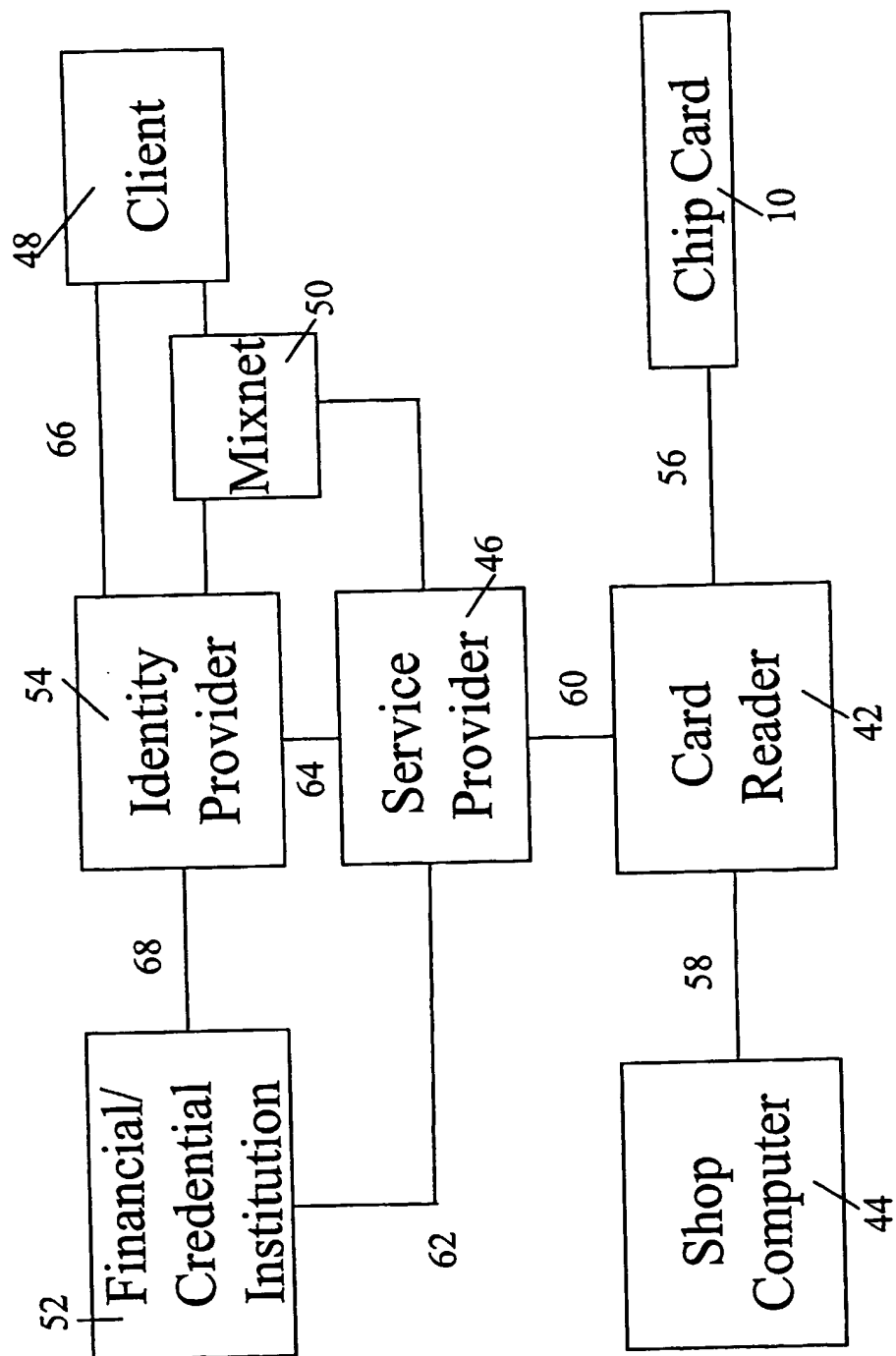
HOME

22. HOME Chipcard

24. Home Communication Device

INFRASTRUCTURE

20. Anonymiser / Mixnet

18. Id Units

16. PRP - Privacy Reference Points

14. Virtual Chipcards

MOBILE   POINT OF CONTACT

12. Communication Device

10. Chipcard

Fig. 2   Privacy Product Tags
              RFID Privacy lifecycle

MOBILE

20. Communication
Device

10. Chipcard

26. Producer Supply Chain

28. Store

30. PRP Privacy Agent

36. Anonymiser / Mixnet / Id Service

38. HOME Chipcard

40. Product recycling

32. Product Tag visible

34. Product Tag Privacy Enabled through
Zero-knowledge Device Authentication

Fig. 3

Privacy Infrastructure

Fig. 4　　　　Basic relation

```
                    Client  48

                    |
                  Mixnet  50
                    |
   Service
   Provider  46
        |
        120
        |
   Card
   Reader  42        Chip Card  10
        |          56
        58
   Shop
   Computer  44
```
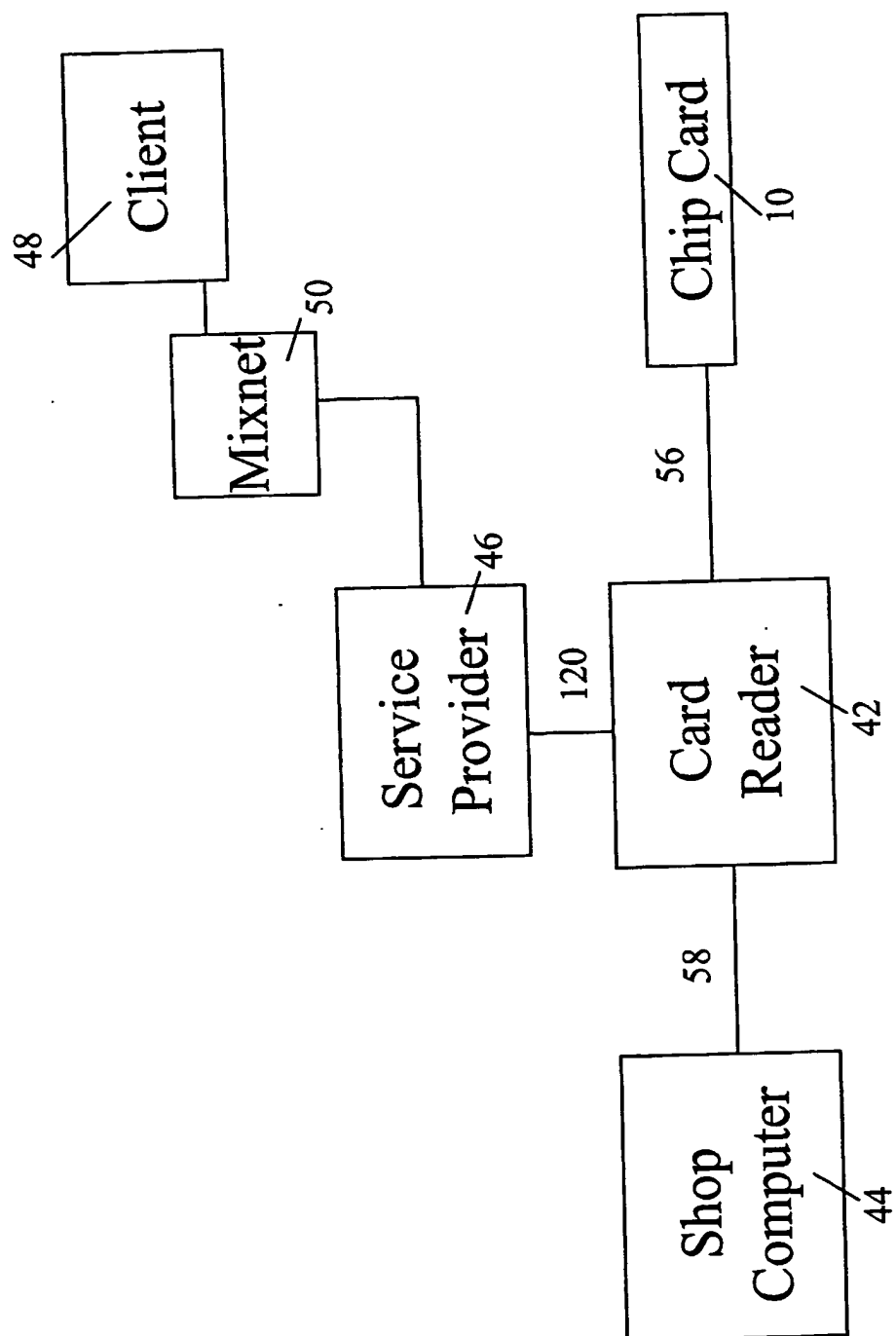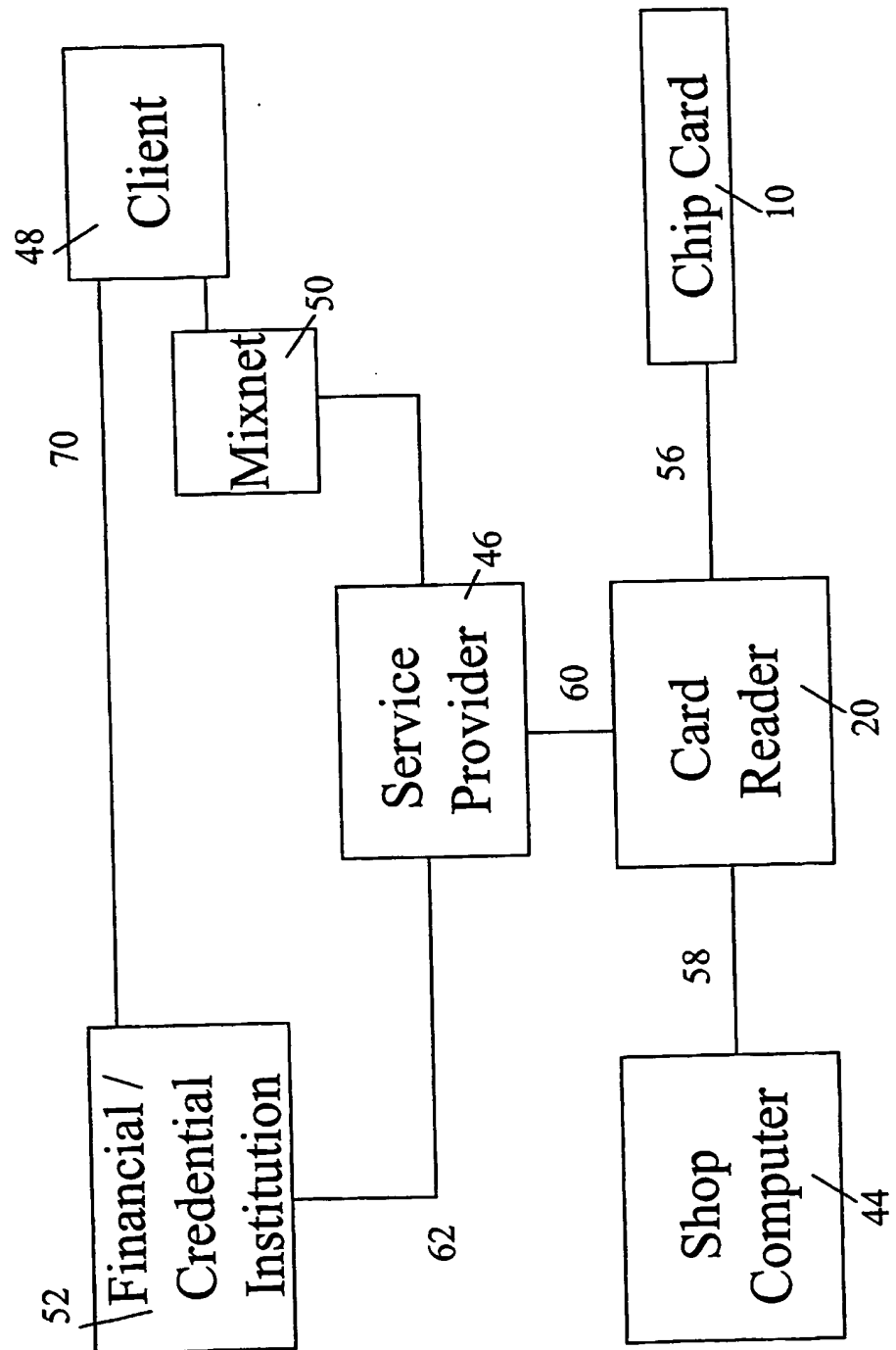
Fig. 5

Managed payment support
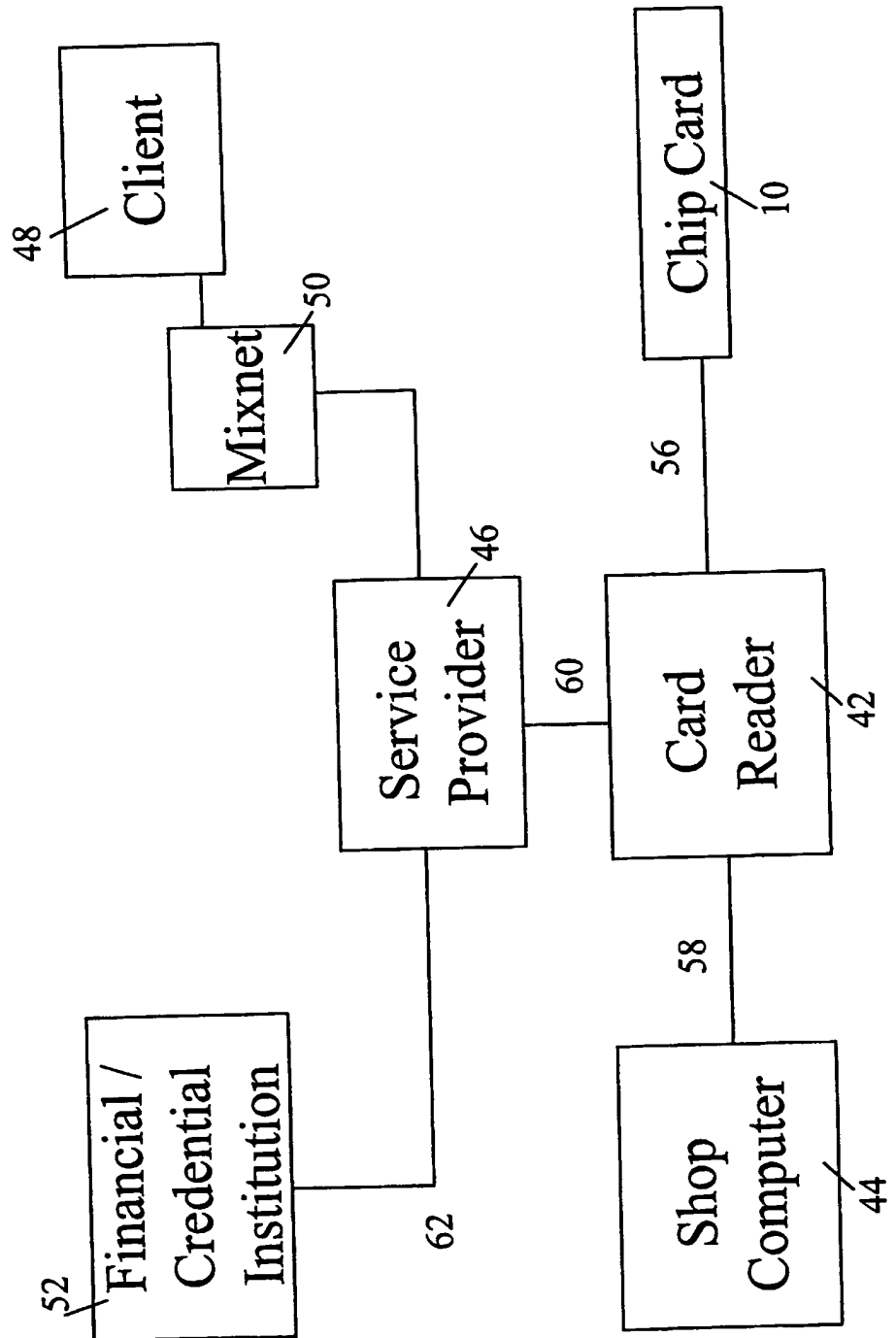
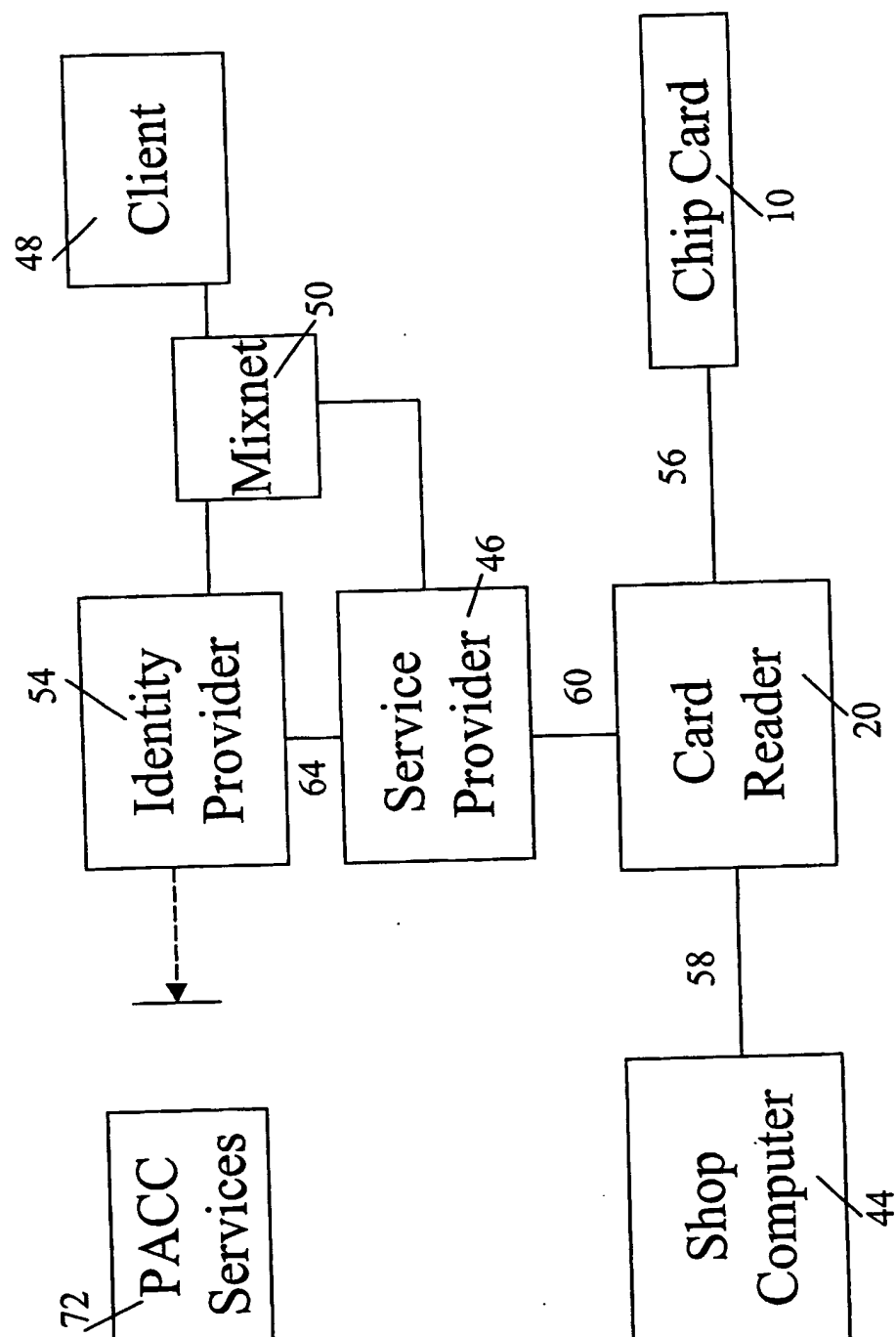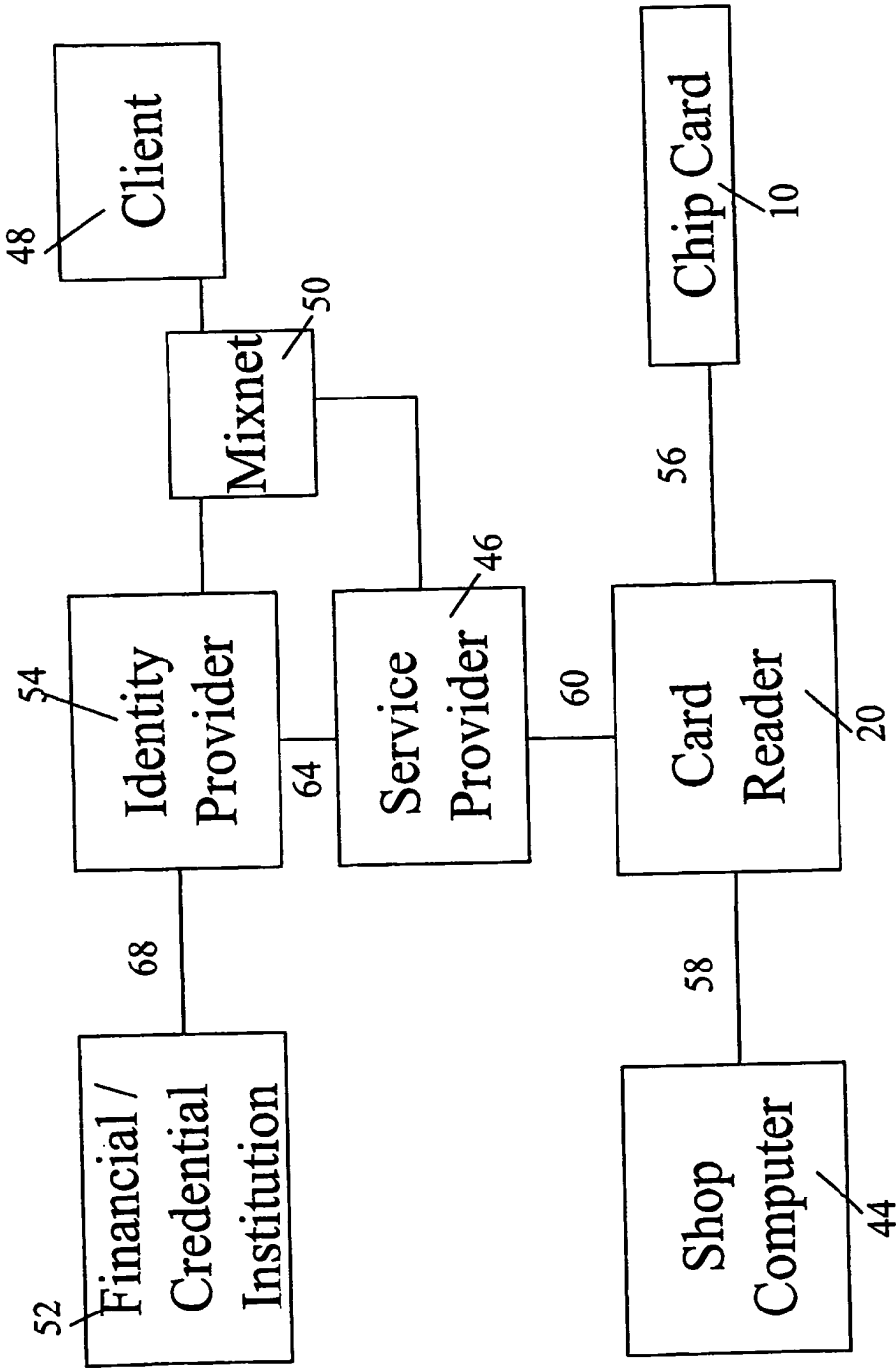Fig. 6   Anonymous Credit

Fig. 7   Basic accountable relation

Fig. 8   Privacy Credit Card

Fig. 9   Privacy Management

Fig. 10　　Device Authentication

Standard PRP processes
Device Zero-knowledge
Device only known at
Point-of-Purchase

Pure Pseudonym based
NO DIRECT Device Access
PACC Optional

Id mgt/
Mixnet

HOME/TRUSTED
SPACE

MAD – Master
Authentication Device

MCD - Master
Communication Device

SMD – Specific
Master Device

SD – Slave Device

VDR - Virtual Device References
<PRP>.VSMD
Each virtual device different key
No reuse between boundaries

Manufacturer can verify new
Hardware-based VDRs using
Blinded signatures and credentials

Group Privacy
Device Authentication
using one-time-only
tickets

Fig. 11 Managed Digital Signature

MOBILE   POINT OF CONTACT   INFRASTRUCTURE

76. Access one-time-only encrypted copy of signature decryption key

82. Forward signature

78. If authenticated and chip card not revoked return data

12. Communication Device

10. Chipcard

Mixnet

74. CA/Signature Unit

80. Optional server-side support
Server.side private key management
With authentication to trace
CA impersonating Client
Mixnets and blinding can shield the session from third party
Advantage:
Signature PKI independent of CA authentication

14. Virtual Chipcards

16. PRP - Privacy Reference Points
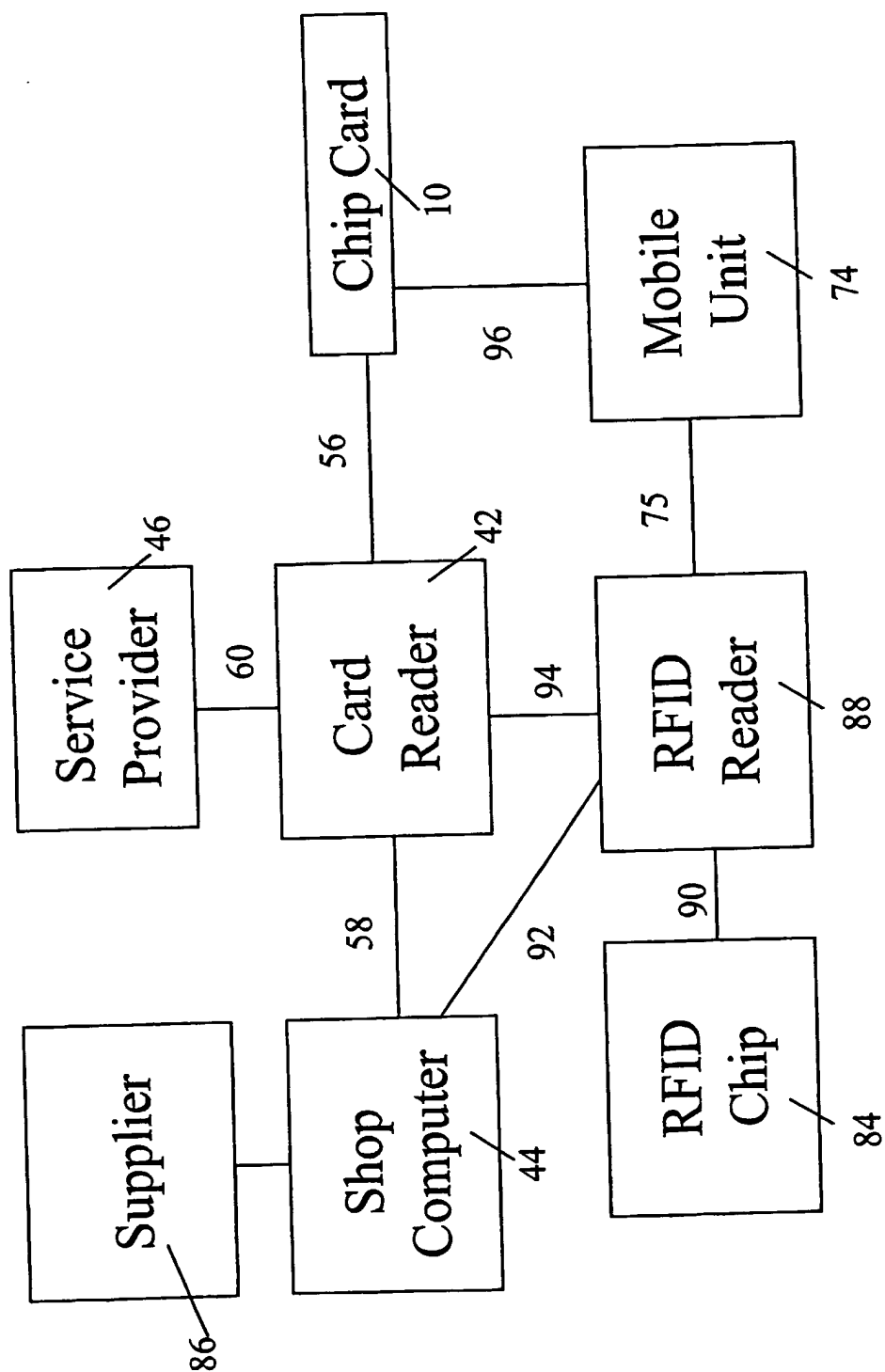
Fig. 12 RFID Infrastructure
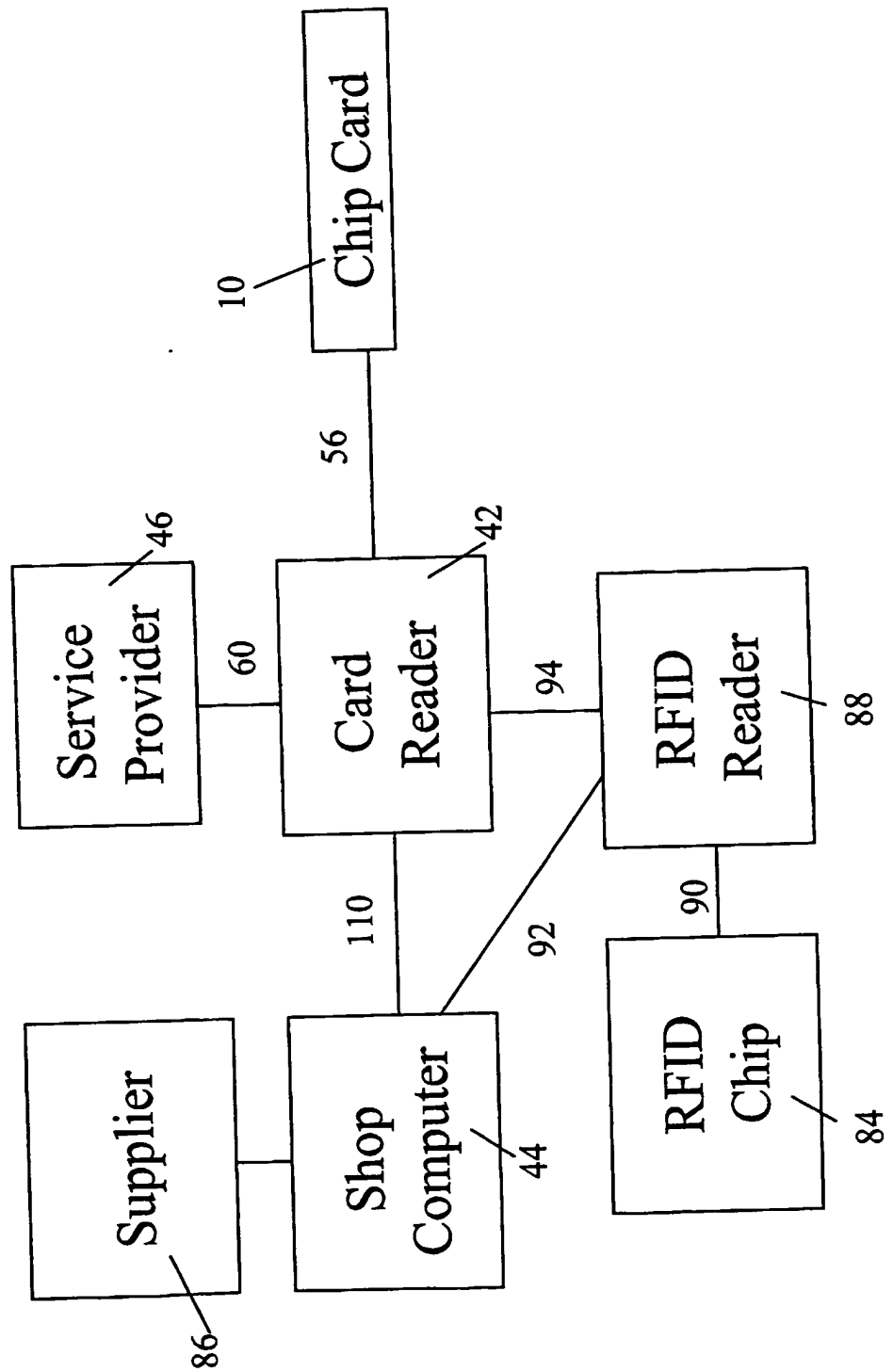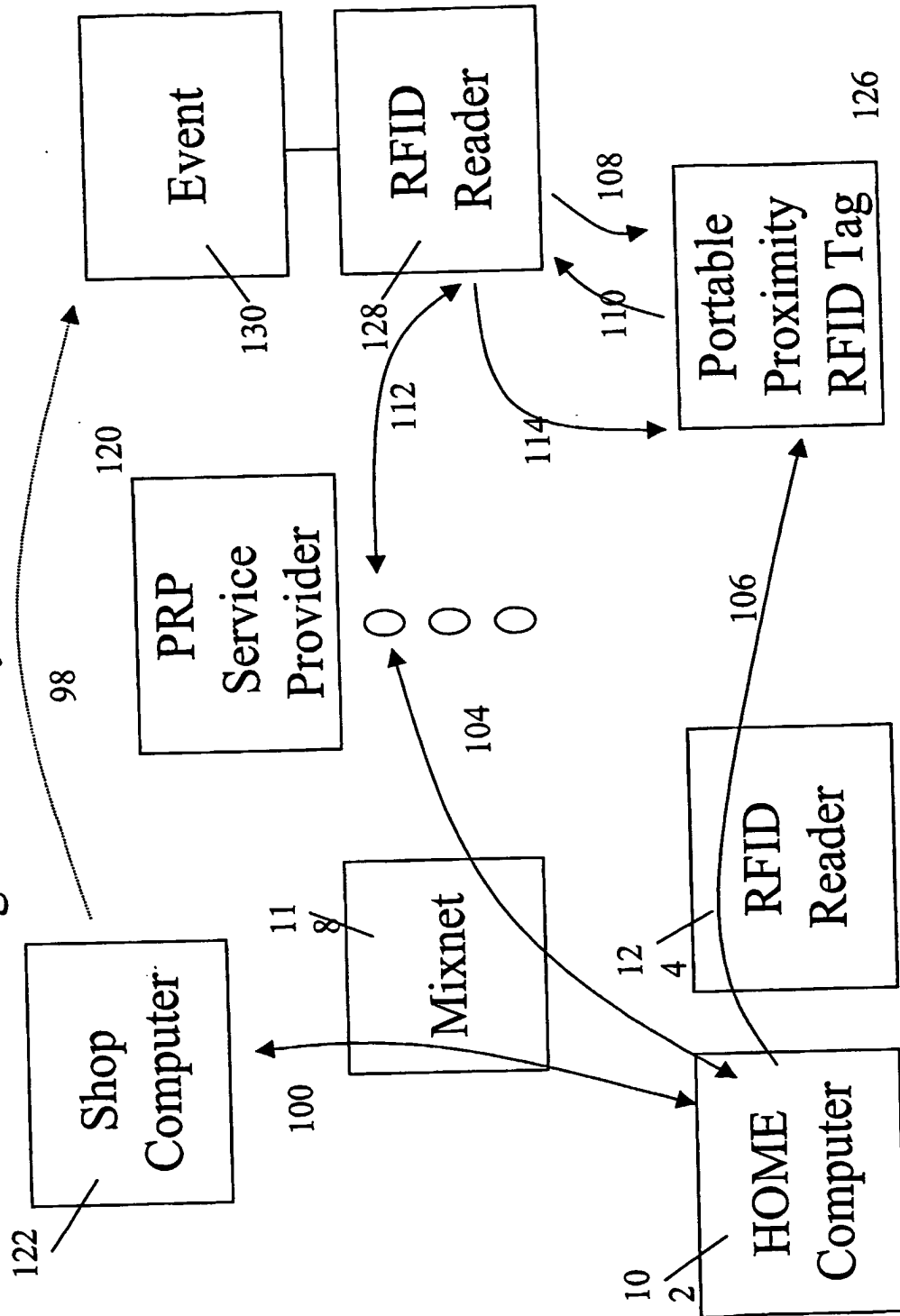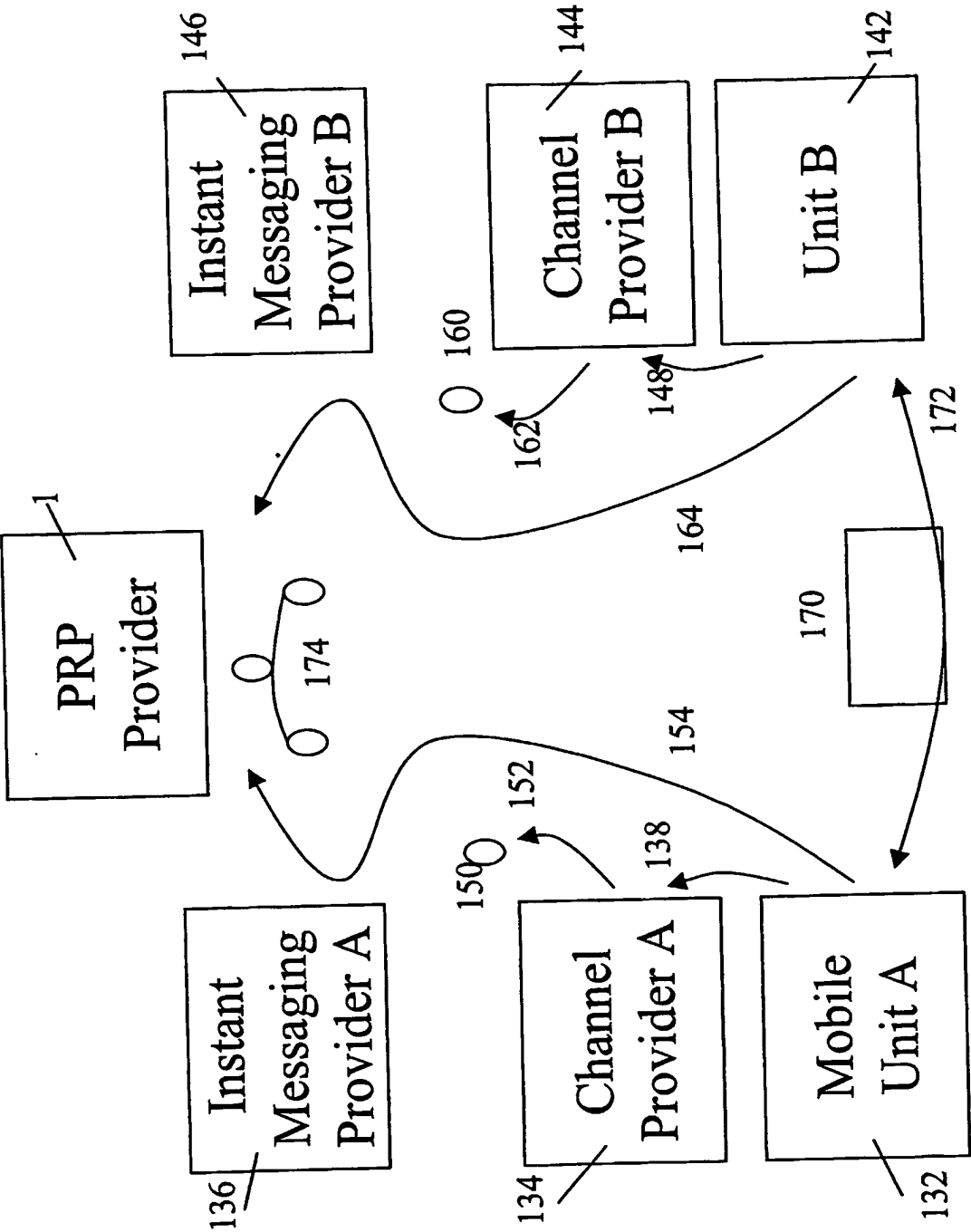
Fig. 13 RFID Authentication

Fig. 14 Privacy Tickets RFID

Fig. 15 Privacy Instant Messaging

Fig. 16   Generic Tag Authentication

Receive Session Authentication Request

Parameter can indicate which key to check against

Check Timestamp Against alive ticket and last successful

If <= last successful and ticket dead → **Ignore (without any response)**

For each key: Validate Authentication

If no more keys → **Ignore (without any response)**

Untested key → **Calculate R (random secret) Validate R against key**

If validation fails →

Success → **Store Session Id and R Store Successful Timestamp If incorporated New Key = f(Key,R)**

Group Key Alive ticket → **Return Session Ack + Ticket shielded with R**

Group Key Create ticket → **Return Session Ack + Next PRP shielded with R Await ticket command**

Device Authentication → **Return Session Ack Await device command E.g. Authenticity authentication**

Group Authentication without ticket → **Return Ack + next one-time-only identifier encrypted with R**

Note:
In production a session timeout is implemented to protect against vaste of one-time-only responses due to traffic jam etc.

Fig. 17 Mobile Privacy